CONFIDENTIAL SUBMISSION

August 27, 2024

To Whom It May Concern:

From September 2021 until February 2024, I was Global Head of Government Affairs at Conduent, a public company that is earning tens of millions of dollars from contracts supporting Maryland's health and human services operations. I am writing to report misconduct by Conduent that has directly impacted Maryland's most vulnerable families. **I respectfully request that the State keep my identity confidential in any investigation conducted in conjunction with this report. To that end, I ask that the State not provide Conduent the documents that I am including with this submission or otherwise provide any indication to Conduent of the source of the information contained in this submission.**

In particular, I know that Maryland leaders have been concerned by the State's Pharmacy Benefit Management (PBM) system's performance problems and security of Electronic Benefit Transfer (EBT) payments. Conduent is the State's contractor for both PBM and EBT operations. I share Maryland leaders' concerns and am writing to ensure that you are aware of additional facts that may help inform State efforts to prevent harm to and strengthen protections for Maryland's most vulnerable families.

1. Pharmacy Benefit Management – Medicaid Participants' Medication Denials

Conduent was awarded its current contract for Maryland's PBM program by the administration of former Maryland Governor Larry Hogan. The contract, under which Conduent provides prescriptions to State Medicaid participants, is valued at more than $72 million.[1] In 2022 Conduent implemented a new PBM system that was inadequately tested and included multiple coding errors. As a result, thousands of Maryland Medicaid participants' prescriptions, many for antipsychotic medicines, were incorrectly denied. Conduent's response to its PBM system errors has been to obfuscate the seriousness of its performance issues and impacts, and knowingly fail to invest sufficient resources in getting Medicaid participants back on their medicines and to prevent future incorrect denials. Company leadership repeatedly has prioritized corporate damage control and its lower costs over protecting public safety.

Mu understanding of the key facts is as follows:

- On January 21, 2023 Conduent discovered that its Maryland PBM system had been incorrectly denying antipsychotic medicine prescriptions for Medicaid participants. These denials began on November 7, 2022 and hundreds of Maryland Medicaid participants had already been impacted by the time Conduent realized the system defect.

[1] *See* Board of Public Works, Oct. 16, 2019 Meeting Documents, at pp. 69-70 (initial PBM contract award to Conduent priced at $73,068,669), 2019-Oct-16-Agenda.pdf (maryland.gov); Board of Public Works, July 7, 2021 Meeting Documents, at pp. 198-201 (decreasing the PBM contract price by $667,045 due to reduced video cost components), 2021-Jul-7-Agenda.pdf (maryland.gov).

- Conduent started using a workaround to prevent more incorrect denials of antipsychotic prescriptions on January 21, 2023, but did not inform the State of the denials at that time. Company leaders reasoned that they did not need to inform the State until its IT personnel had identified the specific line of defective code that caused this impact.

- Rather than promptly reach out to pharmacies to reverse prior incorrect prescription denials, Conduent, instead, focused its resources on conducting an internal assessment of each impacted Medicaid participant's medical records to see if those wrongfully denied State coverage were able to get antipsychotic medicine another way – by self-paying or by getting a sufficiently equivalent alternative prescribed by their doctor.

- On February 17, 2023 Conduent orally informed Maryland state officials that the company identified a coding error in its PBM system. The company did not specify the impact of this error on Maryland Medicaid participants' ability to attain antipsychotic medications.

- In a Root Cause Analysis emailed to Maryland Department of Health officials on February 20, 2023, Conduent stated that the "Date of Incident Identification" was February 16, 2023, which was the date when the company pinpointed the specific line of code causing the incorrect prescription denials. I have enclosed this email for your reference. To my knowledge, Conduent never revealed that company leaders actually learned of the system malfunction and prescription denials several weeks prior.

- Two weeks later, Conduent submitted a written description of the error impacts that was limited to the subset of Medicaid participants (69 members) who were denied prescriptions *and* were unable to self-pay or attain a sufficiently equivalent alternative. This description was emailed by Kim Rankin, Senior Director, Pharma Benefit Management Service Delivery, to the Maryland Department of Health on March 3, 2023. In particular, I believe Deputy Medicaid Director Tricia Roddy received the email; I saw the text but was not on this email.

- Conduent did not conduct any outreach to reverse incorrect antipsychotic medication denials until March 3, 2023. Thus, *nearly four months passed* between when Conduent's PBM system started incorrectly denying prescriptions and when the company started outreach to reverse those wrongful denials. This meant a number of Medicaid participants suffered from being denied antipsychotic medicines for multiple weeks or even months. Such denials could have severe health consequences.[2] Multiple Government Affairs team members were struck by Conduent's callous lack of urgency in responding to risks for Maryland Medicaid participants and those interacting with them. I agreed and internally escalated the need for more company resources for these efforts, to no avail.

[2] *See generally* Nicholas Keks, Darren Schwartz & Judy Hope, *Stopping and Switching Antipsychotic Drugs*, 42 Australian Prescriber 152 (2019) ("Withdrawal syndromes, relapse and rebound can occur if antipsychotics are discontinued, especially if they are stopped abruptly.").

- Conduent's Operations leaders acknowledged that the Maryland PBM system likely had more errors than the one detected so a system audit was launched.
- While it was widely known that Conduent's internal Operations and IT staff members were "swamped," Conduent leaders opted to staff the PBM system audit internally, rather than outsource the work to an external firm. The inadequacy of this approach was apparent as the due date for audit completion slipped repeatedly, from July 2023 to, ultimately, December 2023. See, e.g., my enclosed email to Human Resources Vice President Mariann VanBuren. I was told that Conduent leaders were concerned that hiring an external firm instead might result in findings outside of the company's desired, narrowly tailored scope and could result in greater liabilities for Conduent in Maryland and other states.
- Conduent's outreach efforts to Maryland Medicaid participants who were incorrectly denied medicines, similarly, were woefully insufficient and under-resourced. By the end of May 2023, Conduent had identified 7 different Maryland PBM coding issues implicating 3,235 Medicaid participants' claims by late May, but the company had resolved only 18 percent of those impacted claims due to understaffing on the project.
- A further cause for my concern was how Conduent leadership attempted to misrepresent the Company's PBM conduct to the State. In drafting a reply to a Maryland Department of Health Notice to Cure dated August 24, 2023, which required Conduent to correct multiple PBM issues,[3] Lydie Quebe, General Manager, Government Healthcare Solutions, mischaracterized Conduent's PBM efforts. Her draft text stated that Conduent had qualified employees in all open PBM account positions and that Conduent's teams quickly resolved identified PBM issues. In fact, Conduent lacked qualified employees in multiple critical positions and delayed taking steps to get many Medicaid members back on their medications. I quickly rewrote Ms. Quebe's response to the Notice to Cure and raised concerns about the misrepresentations to other Conduent leaders. See, e.g., my enclosed email to then-Government Solutions President Mark King.
- Conduent never appeared to learn from its mistakes. Given PBM implementation problems, I urged that Conduent perform more testing before implementing any updates to its PBM system. Unfortunately Conduent's leadership again failed to heed calls for more resources, and not surprisingly, new problems surfaced after Conduent made system updates in early 2024. On January 8, 2024, I learned via email that Conduent's updates to the Maryland PBM system had resulted in the denial of mental health prescriptions for 289 Medicaid participants. On February 13, 2024, business owners sent out emails indicating more flawed

[3] This Notice to Cure was conveyed by Chukwuekmeka (Chuk) Okoronkow, Contract Monitor, at the Maryland Department of Health on August 10, 2023.

updates had caused denial of 1,046 antipsychotic medicine prescriptions for 647 state Medicaid members between January 23 and February 13, 2024.

I encourage you to investigate Conduent's disclosures regarding its PBM system errors, its outreach to impacted Medicaid participants, and what it has done to prevent additional harm. Conduent groups that would have significant information would include Government Healthcare Solutions, Government Affairs, Government Operations, Legal, and the Office of the CEO. It could be especially helpful to look at documentation and communications (including emails, texts, and chat messages) concerning this issue sent or received by Mark King (then-President of Conduent Government Solutions, who resigned the end of 2023); Lydie Quebe (General Manager, Government Healthcare Solutions); Chris Malley (Chief Operating Officer, Government Operations); Shankar Balakrishnan (Vice President, Client Partner and Product Strategy, Government Healthcare Solutions); Marianne VanBuren, VP, Human Resources; Kim Rankin (Senior Director, Pharma Benefit Management Service Delivery); Tom Peoples (Pharmacy Solutions Liaison); and me. (There are Conduent Legal Department leaders that may have documentation too, but I am omitting them because the company will no doubt assert privilege over documents flowing to/from these custodians.)

2. Electronic Benefit Transfer System – Data Breaches and Thefts

As you may know, the Maryland Board of Public Works recently approved a $20M contract to renew Conduent as the State's EBT vendor.[4] Through the EBT system, eligible Maryland constituents are issued a card to access State supplemental nutrition and cash benefits. I believe there are facts that the State should be aware of as it evaluates Conduent's recent and future performance as the contractor responsible for overseeing payments to vulnerable families.

A. Conduent employees' thefts from EBT recipients

- Starting in 2022, Conduent customer service representatives stole identity information and government funds from more than 2,500 vulnerable EBT recipient families across 18 states, including Maryland. Maryland victims of these thefts included more than 40 EBT recipient families, with Conduent employees' thefts in the state occurring for nearly a year before the company detected them. A summary of these EBT data breaches and thefts is enclosed in the attached presentation made to Conduent's CEO on December 8, 2023. Conduent leadership learned of the breaches and thefts in September 2023.

- Despite State data breach laws requiring speedy notice of such an event, Conduent delayed providing any notice of the breaches and thefts to impacted State agency clients, including Maryland, for nearly three months, even though the company quickly realized there were significant constituent impacts across multiple states. Conduent leaders offered no good faith basis for delays in informing State clients and in starting joint planning for constituent

[4] Board of Public Works, July 3, 2024 Meeting Documents, at pp. 178-82 (total EBT contract award to Conduent priced at $20.0 million), https://bpw.maryland.gov/MeetingDocs/2024-Jul-3-Agenda.pdf.

notices and repayments. For Maryland, the initial notice was provided in the form of a mid-level Conduent Operations associate sending an email to (only) the Maryland DHS EBT Program Manager on December 18, 2023. I have enclosed this email for your reference.

- The December 18, 2023 email attached a one-page "Final Incident Report" that is confusing in several aspects. First, the word "final" in the title suggests there were prior Conduent communications about the breaches and thefts, when there were none. Second, the "Date of Submission" is listed as December 8, 2023, when in fact the report was sent 10 days later as officials were departing for winter holidays. Third, the "Incident Date/Time" is listed as "9/25/23-12/6/23." This date range represents the dates between when Conduent learned of the thefts and internally investigated without notice to government officials, rather than when the data breaches and thefts occurred. The Maryland breaches and thefts occurred over a longer, earlier time period: between January 23, 2023 and November 16, 2023, a fact acknowledged only in the middle of a Memorandum following the one-page Incident Report.

- In the month following the December 18 email to a single DHS official, Conduent provided no notice or offer of free credit monitoring to Maryland EBT recipients who were the victims of its thefts. I am not sure if/when Conduent provided this constituent notice since then, or if/when Conduent reimbursed the state/constituents for government funds stolen by its employees. I also am unaware of any notice of the EBT data breaches being provided to the State Office of the Attorney General, as required by Maryland statute. In any event, it seems unlikely that any such notice could be sufficiently timely given Conduent delayed notifying its State agency partner of the breaches for nearly three months.

- Conduent was eager to avoid public attention of these long-undetected internal data breaches and thefts, especially as the company sought to renew its Maryland EBT contract. Conduent's Government Affairs team was instructed to not inform any states' leadership of what occurred – even though significant ongoing security risks remained in certain states. See, e.g., the enclosed email from Sean Collins, Vice President of Public Relations and External Communications, in which he emphasized that Conduent only would address the issue "reactively" (i.e., only if asked). I notified Conduent's General Counsel of issues regarding the company's approach in emails in January and February 2024, but I am declining to share that correspondence out of concerns of violating attorney-client privilege.

B. Prevention of third-party EBT thefts

- On February 26, 2023 Conduent CEO Cliff Skelton and then-Government Affairs President Mark King had a call with Secretary of Human Services Rafael Lopez where they informed him that Conduent could make Maryland one of the first states to move Supplemental Nutrition Assistance (SNAP) funds off magnetic stripe EBT cards and onto more secure EMV chip cards. Their meeting talking points included the statement that Conduent believed it could transition SNAP funds to EMV chip cards within a year of State approval of this

contract modification. In mid-2023 I was surprised to hear from Conduent's IT team that this would be impossible – a fact that senior business leaders at Conduent should have known. IT associates explained that Conduent, unlike its primary EBT competitor, had adopted a "single tenant" approach to setting up its EBT platforms, and that Maryland was on the most outdated platform of all Conduent's EBT states. This EBT platform would need to be significantly overhauled – a resource and time-intensive project – before the State could begin moving SNAP funds to chip cards with back-office EMV protections.

- EBT security issues had especially large consequences in Maryland because the State has been placing cash benefits (e.g., disability funds) onto the same cards as SNAP funds. Other states, like neighboring Virgina, opted to place cash funds on separate, more secure cards.
- As Maryland reimbursed millions of dollars of government funds stolen off EBT cards, certain Conduent leaders resisted internal calls last year to highlight to Maryland leadership that the company's then-current contract included a provision offering the State the ability – *at no cost to the State* – to move all of its cash benefits onto separate EMV chip cards immediately, which would dramatically and rapidly reduce State benefits thefts and offer government benefit recipients a better payments experience going forward (as they now could use a credit card to pay rent or utilities bills with government benefits, rather have to pay in cash withdrawn from an ATM). Certain Conduent leaders preferred to promote account control "solutions" (e.g., card lock) to escalating fraud – even though company leaders knew that these offerings were far less effective in stopping fraud – because these solutions generated immediate one-time "impact revenue" that improved Conduent's near-term financial results.

In light of the facts above, it could be helpful for you to investigate the timeline of the Conduent employees' EBT breaches and thefts, because it was not made clear by Conduent's correspondence. It also could be useful to look into specifics of Conduent's response. Potential questions to Conduent could include: How did Conduent fail to detect ongoing employee EBT thefts from vulnerable Maryland families occurring for nearly a year? What is the timeline by which Conduent learned of constituent impacts in Maryland and other States? Why did Conduent wait so long to tell Maryland DHS and other States about the thefts – when the company knew there were significant constituent impacts months before its December 18, 2023 correspondence, and it was apparent that constituent outreach and reimbursement plans would be needed?

I also suggest that you request internal Conduent communications regarding data breaches, thefts, and solutions, controls, and processes intended to prevent the same. Conduent groups with documentation related to this inquiry include Engagement and Eligibility Services, Fraud, Government Affairs, Government Operations, Government Payments, Legal, and Office of the CEO. It could be especially helpful to focus on communications (including emails, texts, and chat messages) involving the following individuals: Wade Fairey (General Manager, Government Payments); Sean Collins (Vice President of Public Relations and External

Communications); Denise Adaway (Director, Account Management, Government Payments); Joe Froderman (Senior Director, Government Operations); Kate Viar (Director, Government Affairs); Terri DiCambio (Regulatory Compliance Consultant, Data Privacy Office), and me. (There are Legal leaders involved too, but I am omitting them because Conduent will no doubt assert privilege over documents flowing to/from them.) You also could benefit from speaking with Chris Jacobson, who was Senior Manager of EBT Fraud Analytics and Claims at Conduent but left the company for another job earlier this year.

I am sharing the information above with you because Maryland is my home state. However, I also encourage you to share your findings with other States as you deem appropriate. For your reference, other States impacted by the Conduent employees' EBT data breaches and thefts (and similarly noticed by Conduent on December 18, 2023) include the following: Alabama, Arkansas, Connecticut, Georgia, Iowa, Indiana, Massachusetts, Maine, Mississippi, New Jersey, New York, Ohio, Oklahoma, South Carolina, Tennessee, Utah, and Virginia.

Please feel free to reach out to me if any additional information would be helpful. My personal contact information is as follows: 240-620-9091 (cell) and jenniechandra@gmail.com.

Sincerely,

Jennie Chandra

Attachments

ATTACHMENTS

Chandra, Jennie

From: Miller, Ed (External)
Sent: Tuesday, February 21, 2023 11:07 AM
To: Athos Alexandrou -MDH-; Ogunremi, Christiana; COTTON, SHELLY; Rankin, Kimberly
Cc: Joseph Smith -MDH-; Chukwuemeka Okoronkwo -MDH-; Dixit Shah (DHMH)
Subject: RE: [External] - Status of Post Go-Live Issue #206
Attachments: Issue 206 - Antipsychotics Grandfathering Impact Analysis v1.xlsx; Conduent RCA - MD GrandFathering Business Rule.docx

Follow Up Flag: Follow up
Flag Status: Flagged

Athos,

Attached is the RCA for issue 206. I have also included a spreadsheet which documents the impacted prescriptions along with the drugs and participants. There were 321 claims and 177 participants impacted. The team is currently reviewing the impacted claims to determine if the participants received an alternate drug on a subsequent claim. Outreach approach discussions are also underway to address getting prescriptions filled for participants that still require medication.

The test results for the modification to fix the issue are currently under review. We will send those over shortly for review / approval.

Once the issue is fixed in production, we will provide an updated impact analysis through the time of the implementation in production.

Please let me know if there are any questions. Thanks.

From: Athos Alexandrou -MDH- <athos.alexandrou@maryland.gov>
Sent: Tuesday, February 21, 2023 9:24 AM
To: Miller, Ed (External) <Ed.Miller@conduent.com>; Ogunremi, Christiana <Christiana.Ogunremi@conduent.com>; COTTON, SHELLY <SHELLY.COTTON@conduent.com>; Rankin, Kimberly <Kimberly.Rankin@conduent.com>
Cc: Joseph Smith -MDH- <joseph.smith2@maryland.gov>; Chukwuemeka Okoronkwo -MDH- <chukwuemeka.okoronkwo@maryland.gov>; Dixit Shah (DHMH) <dixit.shah@maryland.gov>; Athos Alexandrou -MDH- <athos.alexandrou@maryland.gov>
Subject: [External] - Status of Post Go-Live Issue #206

Good morning Ed and Team,

Per our discussion on Friday, you were going to fix New 206 on Friday or Saturday. Furthermore, you were going to determine the impact of this defect on the MD Medicaid participants, as well as devise a plan of action on how to get the impacted participants their medication(s), if appropriate. Finally, you were going to send the RCA.

Can you please provide an update on this? I mentioned it this morning to the Deputy Secretary and they need this information immediately.

Thanks,

--

Athos Alexandrou
Director
Office of Pharmacy Services
athos.alexandrou@maryland.gov
(410) 767-5369

Maryland Department of Health is committed to customer service. Click here to take the Customer Satisfaction Survey.

We encourage you to check our website and social media often for updates.
For Medicaid-related Coronavirus updates, visit mmcp.health.maryland.gov.
For questions about the Coronavirus, visit coronavirus.maryland.gov.
Follow us @MDHealthDept facebook.com/MDHealthDept and twitter.com/MDHealthDept.

Root Cause Analysis

Maryland Point of Sale ("POSECMS")
Grandfathering issue impacting claims adjudication

Date of Incident Identification: 02/16/2023

Date of last update: February 21, 2023
Document Version: 1.0

Preface

This document captures key events and the Root Cause Analysis ("RCA") related to the Maryland Point of Sale ("POSECMS") Grandfathering issue impacting claims.

Scope of systems covered in this document:

- Maryland Claims adjudication system

Contents

1. Incident Summary

System Impact and Business Impact

Background:

Mental Health Grandfathering business rule based on 90/120 days of supply was designed to be implemented in MD Medicaid claim processing. All non-preferred drugs in the AHFS classes mentioned below are to be grandfathered. Grandfathering allows indefinite continuation of prescriptions for the same chemical entity, regardless of dosage strength, if the recipient has received at least one prescription for the drug in the previous 90/120 days.

The 90-day criteria apply to the following AHFS classes:

1. AHFS Class No. 120400 (Cholinergic Agents) donepezil, galantamine, rivastigmine tacrine
2. AHFS Class No. 120804 (Anti-Parkinson)
3. AHFS Class No. 281208 (Benzodiazepines)
4. AHFS Class No. 281292 (Miscellaneous Anticonvulsants)
5. AHFS Class No. 281604 (Antidepressants)
6. AHFS Class No. 282000 (Anorexigenic Agents and Respiratory and Cerebral Stimulants)
7. AHFS Class No. 282408 (Anxiolytics, Sedatives and Hypnotics – Benzodiazepines)
8. AHFS Class No. 282492 (Miscellaneous Anxiolytics, Sedatives and Hypnotics)
9. AHFS Class No. 289200 (Central Nervous System Agents, Miscellaneous)
10. AHFS Class No. 281608 (Antipsychotic Agents)
11. AHFS Class No. 282000 (Anorexigenic Agents and Respiratory and Cerebral Stimulants)

The 120-day criteria apply to the following atypical antipsychotic therapeutic classes:

1. H7T
2. H7X
3. H7Z
4. H8W

As part of the Quality Management and Compliance Audit processes, the Conduent team identified Grandfathering business rule logic was not working as per the initial design.

Business Impact:

Claims for Medicaid members were denied as "Prior Authorization Required" due to an error in the configuration of the FlexibleRx Grandfathering business rule. Hence, the prescribers had to contact call center agents requesting prior authorization for the denied claims.

The claims were denied using exception code 4381 indicating that a prior authorization was required.

Trend report: Overall comparison of claims denied between old vs new system for exception 4381:

System	Month	Claims#
OS+ (old system)	Jun-22	37,312
OS+ (old system)	Jul-22	31,189
OS+ (old system)	Aug-22	35,647
Flex Rx (new system)	Nov-22	34,126
Flex Rx (new system)	Dec-22	35,359
Flex Rx (new system)	Jan-23	36,009

Observation: No significant deviation in claims denial volume for exception 4381

- Individual claims that were improperly denied due to exception and NOT subsequently paid via Prior Authorization – **321**
- Total unique Medicaid members impacted - **177**

Impact:

Due to the error in the look back criteria of the Mental Health business logic in FlexibleRx, claims were incorrectly denied with exception code "4381- Prior Authorization Required". The Mental Health grandfather business logic look back period was incorrectly set at two times the days supply on the claims rather than 90/120 days depending on the mental health medication criteria. The correction for the Mental Health Grandfather business logic has been tested in SIT and additional testing conducted in User Acceptance Testing (UAT) environment. Upon the completion and approval of the test results by MD, the updated business logic will be promoted to the FlexibleRx production environment.

2. Incident Details

Details

The Conduent QMCA program has been analyzing the unexpected increases to the fax/call volumes. This analysis identified an issue with the Mental Health Grandfather business logic. Examples were identified and researched by Conduent and it identified that the look back period in the business logic was only using two times the days supply on the claims instead of 90 or 120 days, based on the mental health drug.

Root Cause

MD Medicaid claim processing business logic was incorrectly using two times the days' supply on the claim instead of a look back of 90/120 days.

Preventive/Corrective Actions

MD FlexibleRx business logic is actively being tested in both the Test and UAT environments. Test results will be given to the MD for approval before the business logic correction is moved into the MD FlexibleRx production environment.

Preventive Action:

1. Test cases will be strengthened to evaluate the workflow of the business logic for both positive/negative paths.
2. Business and/or clinical review of the test cases is conducted as an additional quality assurance measure that all aspects of the business logic are tested.

Chandra, Jennie

From: Chandra, Jennie
Sent: Monday, July 17, 2023 8:02 PM
To: VanBuren, Mariann
Subject: FW: MD June Outage RCA
Attachments: MD_RCA_CNDT-INC1978895_KR.docx

FYI, more news on MD PBM attached. First I've heard of this outage impacting 1,600+ claims last month. I really think Mark should request an "update" meeting on MD PBM with you, Lydie, Chris, their reports, Mike Genchi, and me. Since our last group meeting was on 5/31 and the MD PBM audit was supposed to be completed within 2 months, now is an especially appropriate time for Mark to check in on the status of various efforts in support of this contract.

From: Rankin, Kimberly <Kimberly.Rankin@conduent.com>
Sent: Monday, July 17, 2023 7:45 PM
To: Genchi, Michael <Michael.Genchi@conduent.com>
Cc: Rankin, Kimberly <Kimberly.Rankin@conduent.com>; Chandra, Jennie <Jennie.Chandra@conduent.com>
Subject: MD June Outage RCA

Mike –
Attached is the MD RCA for the outage on June 13th. Please advise if you have any concerns with the RCA write up.
Thanks
K

Kimberly S. Rankin
Senior Director, Pharmacy Benefit Management Service Delivery
MLC Certified Medicaid Professional (MCMP-II)
Conduent Health Services Solution Delivery

(M) 804.370.2527

Chandra, Jennie

From: Chandra, Jennie
Sent: Tuesday, August 29, 2023 2:46 PM
To: King, Mark
Subject: PBM Follow Up
Attachments: MDH_POSECMS_CAP_OM_-001_CIO 08212023 - MG 20230822.docx; FL PFM and TPL deck for AHCA.pptx

Hi Mark,

Thanks for taking time out to connect today! A couple data points following up on our call:

- MD PBM – See p.2 of the first attachment for a summary cover letter proposed by GHS leadership in response to the MD PBM Cure Letter. In addition to being factually inaccurate, this letter text evidences a general approach toward GHS client relationship challenges that, in my opinion, does not serve the company's interests well. That is especially the case in this instance, where the state stated that it would be looking to our response to inform its evaluation of "Conduent's intent and capacity to fully perform its contract obligations."

- FL PBM – See the proposed "Why Conduent" deck (second attachment), which we were asked to share with our FL lobbyists in advance of a Conduent meeting to discuss PBM (and TPL) substance with AHCA officials. Although this is likely our only opportunity to talk with agency staff before RFP releases, the presentation does not present a clear case for the special value Conduent can offer that other companies cannot; likewise, I'm not sure what we might want to encourage for inclusion/emphasis (or avoid) in an RFP. Also we just received this yesterday, after Cliff met with AHCA leadership weeks ago.

While I'm communicating directly with various business owners about the concerns above, it is not clear to me which individual(s) ultimately is accountable for the client relationship and/or sales performance, or what I should do if I'm concerned that they are not being sufficiently responsive to significant Government Affairs concerns. I would appreciate your guidance on both.

Safe travels –

Best,
Jennie

Jennie Chandra
Global Head of Government Affairs

CONDUENT

(202) 868-7768
jennie.chandra@conduent.com


Conduent Government
EBT Fraud Discussion
December 6, 2023
CONDUENT

Agenda

- EBT Industry Background
- Occurrence Background
- Findings
- Future Preventative Steps

EBT Industry Background

Industry Environment

- EBT programs, including SNAP and the Pandemic EBT programs, operate on a "closed loop" network administered by the U.S. Department of Agriculture's Food and Nutrition Service (FNS).
- Unlike with the MasterCard, VISA and other "branded" payment cards, EBT card transactions are not regulated under Federal banking law, such as the Electronic Funds Transfer Act or Reg E.
- EBT transactions are governed by regulations promulgated by FNS (the "FNS Regulations") and published at 7 CFR Part 274.
- Servicers such as Conduent are not responsible fraud losses perse or take claims related to fraud

Industry Precipitating Event: Expedited Change to Allow Online Purchases

- FNS pilot for online purchases was in 2019-2020 with implementation planning in 2020
- All EBT states had online transactions up and running March-July 2021
- EBT online requires an online PIN but no CVV (not required by FNS regulations)
- All states/FNS and Conduent moved fast to implement online transaction processing
- Many PSNAP programs did not provide true SSNs, but rather all Zeros.

Occurrence Background

Identification of Issue

- September 25, 2023, a call center associate noticed suspicious activity whereas a work from home associate accessed a client's EBT card, which they should not have accessed, as part of an inbound fraud call.
- A corporate security incident was opened, and the Fraud team engaged
- Operations and Fraud teams, partnered across the org to identify any potential fraud in all EBT programs

Root Cause Analysis:

- Enabling online transactions where card is not present, a pandemic response

  - compounded by -

- Moving associates home, a pandemic response

  - compounded by -

- Visibility to PAN, a pre-pandemic holdover

Result: Suspected internal fraud from nine associates totaling ~$1M

Future Preventative Steps

People:

- ✓ Hired EBT fraud investigator
- ✓ Re-focused existing resources on EBT

Process

- Reviewing and updating Seibel roles
- Reviewing and updating Seibel permissions
- Auditing all CSR and Fraud associates for proper Seibel role and permission

Technology

- ✓ Seibel enhancements
  - Full PAN → Last 4 PAN
  - Audit Trail for L2 and above (full SSN) → Audit Trail Removed
- ✓ Improved back-end scanners to identify future occurrences more quickly
- Partnering with IT to deploy Data Loss Prevention (DLP) reporting

Appendix

Liability for Unauthorized Transaction

- Unlike with Regulation E, there is currently no provision under the FNS Regulations for allocation of the risk of loss among the state, the cardholder, and the card services provider for unauthorized transactions. However, Conduent's EBT contracts frequently contain the following language with respect to maintaining the overall financial integrity of the contractor's EBT system:

  The Contractor shall bear all liability for any losses resulting from errors or omissions including fraud and abuse on the part of the Contractor or its representatives or Subcontractors. These liabilities include, but are not limited to:

  1. *Any duplicate or erroneous postings of benefits or void actions to a Cardholder account;*
  2. *Any losses from funds drawn from an account after the Cardholder notified the Contractor that the card had been lost or stolen;*
  3. *Any losses from transactions performed with cards issued but not activated by the Cardholder and/or the Contractor;*
  4. *Any losses from transactions completed using invalid Retailer FNS authorization numbers or invalid WIC vendor ID's;*
  5. *Any damages or losses suffered by a Federal or State agency due to negligence on the part of the Contractor.*

- In addition, Conduent's EBT contracts frequently require the EBT contractor to maintain systems and controls for the EBT platform that align with the framework of NIST Special Publication 800-53.

Even though Regulation E does not apply to EBT, Conduent is accountable to the state customers to prevent fraud, waste and abuse in general. In other words, we must maintain a comprehensive system of controls in place to manage the various risks of operating the platform. Practically speaking, what that means in today's EBT environment is that we must align with NIST SP 800-53. ***So as Conduent assesses and reports on this incident and describes the various remedial steps we plan to take, we should be using the language and the framework of NIST as much as possible.***

Findings

Scope

- Nine associates were identified as having suspicious activity and have been terminated
- Going back to each date of hire, ~$1M in suspicious activity is identified
  - $524k in PSNAP transactions → leveraged 0 SSNs to identify accounts, leverages full PAN to enable ATO
  - $433k in SNAP transactions → Leveraged full PAN to enable ATO after client call
  - $78k still being determined as PSNAP or SNAP

- 2,182 customers across 18 programs impacted

CONDUENT

BRXXXX

Chandra, Jennie

From: Messer, Keith
Sent: Monday, December 18, 2023 10:00 AM
To: judy.marsh@maryland.gov
Cc: Harmon, Heather; Froderman, Joe
Subject: Conduent Incident Notification 11/9/2023
Attachments: 2023-1771 Individual Notification - Draft 12.12.2023_all programs.pdf; Incident Report 12_8_2023_MD_FinalV1.pdf; Transaction detail.xlsx; State response _V1MD12.8.23.pdf

Good morning, Judy,
Reaching out to you regarding the incident from 11/9/2023. Please find the attached.

1. State Response
2. Incident Report
3. Individual Notification – Draft
4. Transaction detail

If your team could help us with the following:

- How should Conduent handle adjustments to the state, cardholder or back to the state?
- Is there a specific agency Conduent should coordinate with for consideration when legal action is pursued?
- Should Conduent be sending the notification to the cardholders or would the State like to send those out?

Please feel free to reach out to me with any questions, concerns, or comments you might have in regards to this matter.

Best regards,

Keith Messer MSW
Service Delivery Manager (SDM)
Conduent
Nashville, Tennessee
Cell: 615.495.8959
keith.messer@conduent.com

CONDUENT

Final Incident Report – Conduent Payment Services

Report Type: **Report Delivery Date:** **Impact:** **Incident Date / Time**	Final Incident Report 12/8/2023 Maryland EBT 9/25/2023 - 12/6/2023
Source/Cause of Security Incident:	A Conduent customer service representative made unauthorized use of account data to engage in theft of benefits from some SNAP recipients. The employee used PII available to her in her work capacity to re-PIN and take over cardholder accounts, thereafter, using the accounts to make online purchases. Upon exhaustive review, Conduent determined five associates impacting 41 cardholders for a total of $35,222.72 were involved in the incident. Of the 41 cardholders identified 15 cases were identified as having zero's as social security numbers. True social security numbers impacted was 26.
Key Events:	• On 9/25, a Conduent Customer Service Representative identified unusual behavior potentially tying an associate to fraudulent activity. This behavior was reported, and an internal security incident initiated. • This investigation was conducted by HR, Corporate Security, and the Conduent internal Payment Fraud Team, evaluating all transactions for all CSRs for the past six months, ultimately identifying five associates. • All associates' access was immediately restricted, the associates placed on leave, and ultimately terminated. • Suspected associates were investigated to the beginning of their employment, leading to the total impact identified.
Description of Information Disclosed:	Cardholder PII and other information accessible through the EPPIC system, including DOB, SSN and card balances.
Corrective Action and Mitigation:	• The employees have been terminated. • The Conduent Corporate Security Office is engaged and will assist state agencies in pursuing any further investigation. • Fraud personnel and technologies have been updated to prevent future occurrences. • The Conduent service delivery team will coordinate with state agencies to provide appropriate financial reimbursement to the Program. • CRM system enhancements implemented to further tighten data security.

Final Incident Report – Conduent Payment Services

CONDUENT

December 18, 2023

MEMORANDUM

To: State of Maryland Department of Human Services

From: Conduent State & Local Solutions, Inc.

Subject: Contract for Electronic Benefit Transfer (EBT) Services
Professional Services Contract #OTHS/EBT-15-001-A^ dated June 6th2023.

Final notice of security incident

Dear Client,

This notice is provided to you in accordance with the above-referenced contract. The purpose is to provide additional details and final guidance with respect to the security incident involving the misconduct of certain Conduent employees (now terminated) and the apparent theft of benefits belonging to recipients under Maryland Supplemental Nutrition Assistance Program ("SNAP") as initially reported on November 9th.

Conduent takes this matter very seriously and has committed all appropriate resources to ensuring a proper resolution, including making the State whole for financial losses for which Conduent is responsible, and taking steps to mitigate any reoccurrence of incidents of this type in the future through changes in people, processes, and technology.

Based on our evaluation of the online financial transactions, we provide the below response to assist you in understanding our investigation process and the actions we have taken to protect your cardholders:

1. **How were these incidents first detected-**
   On September 25th a cardholder receiving benefits under another EBT state program reported that they believed someone had access to their benefits, even though the cardholder had maintained continuous possession of the physical card.

   Based on this information, the Conduent call center representative evaluated the case in question and identified that one Conduent customer service representative had reviewed the account multiple times.

The Conduent customer service representative determined that the case appeared to look suspicious and reported the incident to Conduent management on the same day that the call was received from the cardholder.

As soon as management received the information from the call center representative, a corporate security request was initiated as well as notification to the EBT fraud manager. Internal investigations were immediately started to determine if internal fraud had occurred and what state or states could be impacted.

Preliminary results of the internal investigation were developed during the week of November 9th 2023, with the investigation as a whole determined to be complete as of December 6, 2023.

Between September 25, 2023 and December 6, 2023, Conduent investigators performed an extensive search of online financial transactions, in this case meaning 1) transactions initiated through the SNAP/EBT online purchasing process, or 2) transactions keyed in at the point of sale without a physical card swipe. This search was conducted to determine:

- whether there were online financial transactions fraudulently performed
- which transactions were made by the cardholder versus transactions made by our CSRs
- whether there were additional customer service agents involved in fraudulent activity.

Based on our search for the time period in question, Conduent identified five associates impacting 41 cardholders totaling $35,222.72 and has provided the final incident notification as part of this final reporting package.

2. **Over what period of time did the conduct occur-**
   Conduent has identified that online financial transactions were impacted from January 21, 2023, to November 16, 2023.

3. **What were the dates of the fraudulent transactions-**
   There were 252 transactions covering the period of January 21, 2023 to November 16, 2023. You will find the attached financial transactions in question per cardholder as part of this reporting package.

4. **What measures has Conduent implemented to ensure that such activity does not reoccur-**
   Conduent has implemented comprehensive corrective actions. These actions have been organized according to people, processes, and technology, as follows:

   People:

   Conduent has hired and installed new leadership within its Payment Fraud team to provide general oversight, make strategic improvements, and engage in knowledge transfer, helping to maintain the currency of the team's overall knowledge and expertise.

   Process:

   - Conduent has updated both the roles and privileges assigned to CSRs under its Seibel Customer Relationship Management (CRM) system.
   - Conduent has conducted an audit for compliance with the updated roles and privileges.

Technology:

- Conduent has implemented specific technology enhancements to its CRM platform:
  - Truncated the card number to display the last 4 digits only on all screens.
  - Removed CSR access to a system-generated audit view within the CRM tool that displayed the SSN of the cardholder for the subject account in specific user roles.
  - Improved internal systemic monitoring.

5. **Does this CSR have any history of performance issues or similar behavior-**
   Conduent maintains the confidentiality of HR matters, but would be willing to coordinate with state officials to arrange for an appropriate confidential review. Conduent fully appreciates the importance of maintaining the integrity of this essential program and we are prepared to respond promptly to any contact from your office.

6. **How does Conduent screen CSRs prior to hire-**
   The Recruitment Team within the Conduent Human Resources Department identifies and screens prospective customer service agents and a background check is performed in accordance with Conduent internal policies. For additional personnel-related information, please see response to Question #5 above.

7. **Has Conduent referred the incident(s) to law enforcement? If so, please provide information about the referral (e.g., date of referral, law enforcement agency)-**
   On December 6th an executive level briefing was completed with the determination Conduent would be coordinating with law enforcement as part of the closure related to this incident.

   Conduent is in the process of finalizing a package of required data evidence that we expect that law enforcement will need in order to complete a thorough investigation. We do not have an exact date at this time, but Conduent will provide customer communications as we work towards law enforcement activities.

8. **The name and address of the employee Conduent has identified as engaging in fraudulent activity-**
   We will gladly facilitate the state obtaining this information and suggest that we connect together with the law enforcement agency to allow the state to learn the specific identity details in due course.

Conduent has attached the following reporting package:

- Final incident report
- All case numbers and dollars impacted.
- Financial transactions identified as fraudulent associated to each cardholder (i.e. case).
- Draft notification that will be sent to cardholders.
- Credit monitoring details for the impacted cardholder accounts.

Conduent will work with you as part of our next steps to determine the appropriate way to credit you or your cardholders' accounts for those transactions identified as fraudulent.

Unfortunately, this issue occurred as a direct result of our desire to provide the highest level of service possible to our partners during the pandemic. Like all States, Commonwealths, and businesses nationwide Conduent needed to react to the situation quickly and establish protocols for employees to work safely from their homes. While this was caused by bad actors, we acknowledge they were our employees and take financial responsibility for their misconduct and apologize to the State of Maryland for the impact to you and your clients. Rest assured no client will bear any financial liability for the loss of benefits.

Please feel free to contact me with any questions, comments or concerns you wish to talk through.

Sincerely,

Joe Froderman
Vice President, Service Delivery
Payment Operations

Conduent State & Local Solutions, Inc.
100 Campus Drive, Suite 200
Florham Park NJ 06108

State logo or Conduent logo here

XX/XX/2023

In connection with your participation in the Supplemental Nutrition Assistance Program ("SNAP") as an EBT cardholder, we are writing to inform you of a privacy incident involving your personal information. Conduent State & Local Solutions, Inc. is a service provider that supports the Insert state and agency name here.

WHAT HAPPENED:

Conduent has learned that the personal information of certain EBT cardholders held in our company's possession may have been exposed in a data security breach. The purpose of this notice is to alert you so that you can take appropriate precautions.

WHAT INFORMATION WAS INVOLVED:

Our investigation determined your name, address and one or more of the following was exposed: date of birth, social security number and Personal Account Number (PAN).

WHAT ARE WE DOING:

We are reviewing our processes and making changes to prevent this from happening again. We are also offering at no cost to you 24-month credit reporting monitoring. Please see attached instructions to sign up for credit monitoring.

WHAT CAN YOU DO:

Please review the attachment to this letter (Best Practices For Protecting Against Fraud) for further information on steps you can take to protect your information and how to receive your free credit monitoring services.

FOR MORE INFORMATION:

We sincerely regret any inconvenience this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care. Please contact us with any questions or concerns at XXX-XXX-XXXX.

Sincerely,

Name and Title

BEST PRACTICES FOR PROTECTING AGAINST FRAUD

We recommend that you always remain vigilant to protect against potential fraud. It is best practice to review your account statements and credit reports closely. If you detect any suspicious activity, promptly notify the financial institution or company with which the account is maintained. You may wish to contact credit reporting agencies to request a fraud alert, credit freeze, or take other actions to monitor your credit.

Consumer Reporting Agencies. You may order a credit report to review your accounts and credit history for any signs of unauthorized transactions or activity. U.S. residents are entitled to one free credit report annually from each of the three major credit bureaus. To order, visit www.annualcreditreport.com or call (877) 322-8228. You may also contact the national consumer reporting agencies:

Equifax	**Experian**	**TransUnion**
Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 800-685-1111	Credit Fraud Center P.O. Box 9554 Allen, TX 75013 888-397-3742	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 888-909-8872
www.equifax.com/personal/credit-report-services	www.experian.com/help	www.transunion.com/credit-help

Immediately report any unauthorized activity on your credit or bank account to your financial service providers. You have the right to file a report with your local law enforcement if you ever suspect you are the victim of identity theft or fraud. You can also file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at (877) 438-4338.

Place a Fraud Alert on Your Credit File. We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	(800) 525-6285
Experian	(888) 397-3742
TransUnion	(800) 680-7289

Consider Placing a Security Freeze on Your Credit File. If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze

https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888)-298-0045

(888) 909-8872

To place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

ADDITIONAL RESOURCES

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the Federal Trade Commission (FTC).**California Residents**: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Maryland Residents**: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **Oregon Residents**: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

EQUIFAX®

Enter your Activation Code: XXXXXXXXXXX
Enrollment Deadline: XXXXXXXX XX XXXX

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of **XXXXXXXXXXXX** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. [2]Credit monitoring from Experian and TransUnion will take several days to begin. [3]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [4]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [5]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co [6]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Chandra, Jennie

From: Collins, Sean
Sent: Wednesday, January 10, 2024 10:53 PM
To: Chandra, Jennie
Cc: Franz, Neil
Subject: RE: EBT Matter and NYC Op-Ed on Parking Equity

Follow Up Flag: Follow up
Flag Status: Flagged

Cliff said we aren't doing that Op-Ed. Feel free to call Tracy on that.

On the EBT matter – once I have approval on the **reactive** statement and accompanying **reactive** Q&A, we'll send it to you. It's to be used **reactively**.

Best,
Sean

From: Chandra, Jennie <Jennie.Chandra@conduent.com>
Sent: Wednesday, January 10, 2024 6:50 PM
To: Collins, Sean <Sean.Collins2@conduent.com>
Cc: Franz, Neil <Neil.Franz@conduent.com>
Subject: RE: EBT Matter and NYC Op-Ed on Parking Equity

Thanks for the update. I'll touch base with Michael/Nicole on both....

From: Collins, Sean <Sean.Collins2@conduent.com>
Sent: Wednesday, January 10, 2024 12:38 PM
To: Chandra, Jennie <Jennie.Chandra@conduent.com>
Cc: Franz, Neil <Neil.Franz@conduent.com>
Subject: EBT Matter and NYC Op-Ed on Parking Equity

Hi Jennie,

Reaching out on a couple of follow ups:

On the EBT matter, at this stage we are not planning to handle that proactively. If you still feel differently, pls reach out to Nicole Bearce and discuss.

On the NYC Op-Ed on Parking Equity – given we are selling the business, Conduent will no longer be working on the op-ed project.

Thanks,
Sean